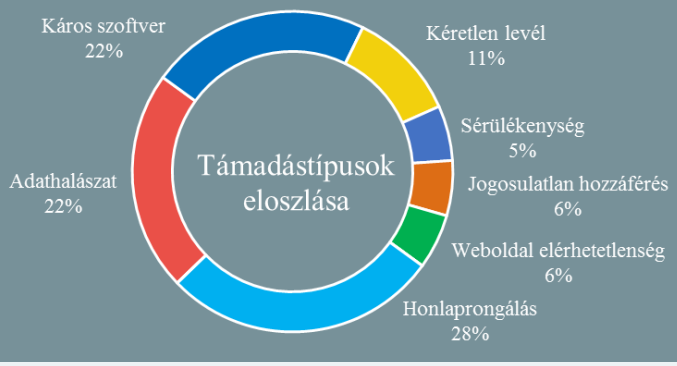
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2019. 34. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.08.16. - 2019.08.22.



Kövessen minket megújult weboldalunkon, ahol friss IT-biztonsági hírek kerülnek publikálásra!

Így reagálnak a böngésző szolgáltatók a kazah kormány internetes megfigyelésére

(techcrunch.com)

A kazahsztáni kormány még korábban kötelezővé tette felhasználói számára a kormány által biztosított gyökértanúsítvány telepítését, amely a kritikusok szerint csupán a HTTPS internetes forgalom közbeékelődéses támadására (MitM), ezáltal pedig az állampolgárok internetes tevékenységeinek megfigyelésére adott lehetőséget. Az Apple, a Google és a Mozilla válaszként egy közös nyilatkozatban jelentették be, hogy különböző technikai megoldásokkal kívánják védeni kazahsztáni felhasználóik adatait, illetve magánélethez való jogukat, így tiltásra kerül böngészőjükből a tanúsítvány. Bár a kazah kormány azóta már nem kényszeríti ki a tanúsítvány telepítését és engedélyezi annak törlését az eszközökről – mondván véget ért az ún. „rendszer tesztelés” -, a Google és a Mozilla ennek ellenére mégis úgy véli, hogy a tiltással megakadályozható a tanúsítvány működése még abban az esetben is, ha az nem kerül eltávolításra az eszközről.

Adatvédelmi konzorcium jön létre a tech cégek között

(www.engadget.com)

A Linux Alapítvány keretei között fog létre jönni a Confidential Computing Consortium (CCC), amelynek tagjai az Alibaba Cloud, az Arm, a Baidu, a Google Cloud, az IBM, az Intel, a Microsoft, a Red Hat, a Swisscom és a Tencent. A projekt célja, hogy meghatározza és felgyorsítsa a nyílt forráskódú ún. „confidential computing” technológiákat, amelyek segítségével a használatban lévő adatok az adatok tulajdonosa, vagy az általuk az adatok megismerésére felhatalmazottak kizárólagos hozzáférését biztosító titkosítás és védelem alatt állhatnak. **Bővebben...**

A Gmail hibaüzenettel válaszolt a bejelentkezőknek

(www.bleepingcomputer.com)

Több felhasználó is jelezte, hogy hitelesítési problémák miatt nem tudtak bejelentkezni Gmail fiókjukba, amelyre a levelező szolgáltató egy hibaüzenettel válaszolt. A Google Cloud Platform státusz dashboard-ja szerint a #19008-as számon rögzített incidensben a Google App Engine, a Google Cloud Console, az Identity Aware Proxy és a Google OAuth 2.0 végpontok érintettek. A Platformon figyelemmel kísérhető volt a hibajavítás folyamata, így látható, hogy az incidens 11 óra 30 perckor került rögzítésre és közel két óra alatt már orvosolták is a problémát. **Bővebben...**

Egészségügyi kutatóközpontok után kémkednek a kínai hackercsoportok

(www.securityweek.com)

A FireEye egy a héten kiadott jelentése szerint továbbra is az egészségügyi kutatásokban résztvevő szervezetek, azok közül is leginkább a daganatos megbetegedésekkel összefüggő (rákkutatás) információk után kémkednek a kínai hackercsoportok, valószínűleg az országban uralkodó daganatos megbetegedési és halálozási arány, valamint az egészségügyi költségvetés miatt. A FireEye jelentésében mindezt azzal is indokolta, hogy a kínai gyógyszeripar az egyik leggyorsabban fejlődő, így a megszerzett információk birtokában képesek lehetnek más nyugati országok előtt piacra hozni a gyógyszereket. **Bővebben...**

Visszakerült egy biztonsági rés az iOS legújabb verziójába

(securityaffairs.co)

Az Apple júniusban adta ki az iOS legújabb, 12.4-es verzióját, amelybe – feltehetően véletlenül – visszavezetésre került egy olyan biztonsági rés (exploit), amit a korábbi 12.3-as verzióban már javítottak. A GitHub-on Pwn20wnd felhasználói néven ismert kutató, aki a múltban fejlesztett már JailBreak-eket iPhone telefonokhoz, nyilvánosságra hozta az iOS 12.4-es verzióhoz fejlesztett kiadását, ami olyan exploit kódot tartalmaz, amivel a támadók képesek lehetnek hozzáférést szerezni az iPhone készülékekhez, viszont erre csak a legújabb iOS verziók esetén van lehetőség. Mindezt több felhasználó is megerősítette, köztük Ned Williamson, a Google Project Zero szakértője is. Az eset szokatlanságát az adja, hogy a sérülékenységek feltárói ahelyett, hogy nyilvánosságra hoznák a sebezhetőségeket, általában az azokért legmagasabb összeget kínáló platformokkal, mint például a Zerodium-mal osztják meg az információkat. **Bővebben...**

IT biztonsági Tanács

Manapság egyre több applikáció biztosít lehetőséget arra, hogy az alkalmazásainkhoz való hozzáférés csak jelkód, vagy - beállítási lehetőségektől, illetve készülékünk tulajdonságaitól függően - ujjlenyomatunk megadásával érhessük el a kívánt szolgáltatásokat.

Ezért az érzékeny adatok tárolására alkalmas kritikus alkalmazásokhoz, például banki és csevegő applikációkhoz, galériához való hozzáféréseket célszerű a készülék feloldási kódjától eltérő jelkóddal korlátozni.

Az Apple késlelteti a gyermekeknek szánt appokra vonatkozó adatvédelmi szabályok módosítását

(www.engadget.com)

Az Apple év elején tartott fejlesztői konferenciáján (WWDC) bejelentették, hogy a kiskorúak védelme érdekében szigorítanak az App Store felülvizsgálati irányelvein, miszerint a „gyermek” kategóriába szánt alkalmazások nem tartalmazhatnak majd harmadik féltől származó hirdetési vagy nyomkövetési eszközöket. A cégnek szeptemberben kellett volna eszközölnie a módosításokat, azonban a The Washington Post szerint későbbre halasztják az új szabályok bevezetését, arra hivatkozva, hogy néhány fejlesztő pontosítani szeretné az elvárásokat annak érdekében, hogy teljes mértékben megfelelhessenek majd az új irányelveknek. **Bővebben...**

Az Egyesült Államokban késleltetik a Facebook új funkciójának bevezetését

(www.bloomberg.com)

Egy Texas állambeli bíró egy prostitúciós célú emberkereskedelmi peres eljárás során ideiglenesen betiltotta a Facebook új, még bevezetés előtt álló Facebookon Kívüli Aktivitás (Off-Facebook Activity) elnevezésű funkcióját. Írországban, Spanyol országban és Dél-Koreában már elérhető az adatvédelmi célú eszköz, amely lehetővé teszi az internetes előzmények felhasználói profiltól való elkülönítést és az előzmények törlését, viszont az Egyesült Államokban mindez még nem került bevezetésre. Egy prostitúciós célú emberkereskedelmi ügy áldozatát a közösségi portálon keresték fel a kerítők, így az áldozat ügyvédei felkérték a Facebookot a gyanúsítottak böngészési előzményeinek átadására, amelyre a közösségi hálózat nem teljesített. **Bővebben...**

Hirdetésekre vonatkozó adatvédelmi szabványok kidolgozását kezdeményezi a Google

(thehackernews.com)

A Google bejelentette új adatvédelmi kezdeményezését, a Privacy Sandbox-ot, amelynek célja olyan nyílt szabványok kidolgozása, amikkel az adatvédelmi aggályok csökkentése mellett, továbbra is támogathatók az online hirdetésekből származó bevételekre támaszkodó webhelyek. A Google blogbejegyzésében elismerte, hogy a személyre szabott hirdetéseket eredményező hirdetéskövetés meghaladta kezdeti célját, viszont megjegyzi, hogy annak adatvédelmi szempontból történő tervezetlen javítása váratlan következményekkel járhat a felhasználóknak, a hirdetőknek és a vállalkozásoknak egyaránt. **Bővebben...**

WebAuthn támogatással egészül ki a GitHub

(www.theregister.co.uk)

A GitHub kibővíti kétfaktoros azonosítási (2FA) lehetőségeit a Web Authentication (WebAuthn) biztonsági szabvány támogatásával. A platform már ezidáig is támogatta a különböző 2FA megoldásokat, mint az SMS üzenetben érkező ellenőrző kódok, az egyszer használatos jelszó alkalmazások (one time passwords – OTP), illetve a U2F (Universal Second Factor) biztonsági kulcsok, amely egy régebbi szabványra épülnek. Ez év márciusában a World Wide Web Konzorcium (W3C) jóváhagyta a WebAuthn specifikációt a FIDO Szövetség (FIDO Alliance) specifikációkészletének, a FIDO2 részeként. A WebAuthn szabványra való áttérés azt jelenti, hogy a GitHub támogatja a fizikai biztonsági kulcsok használatát a Firefox és a Chrome böngészők Windows, macOS, Linux, Android verzióiban, valamint a Safari böngésző macOS és iOS verzióiban. **Bővebben...**